



wifi: cfg80211: cancel pmsr_free_wk in cfg80211_pmsr_wdev_down

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2026-31548
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-24 15:16:28 UTC
Updated	2026-04-27 20:15:55 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: wifi: cfg80211: cancel pmsr_free_wk in cfg80211_pmsr_w

Risk And Classification

Primary CVSS: v3.1 7.8 HIGH from 416baaa9-dc9f-4396-8d5f-8c081fb06d67

CVSS: 3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

EPSS: 0.000240000 probability, percentile 0.067850000 (date 2026-04-27)

Problem Types: NVD-CWE-noinfo

Version	Source	Type	Score	Severity	Vector
3.1	416baaa9-dc9f-4396-8d5f-8c081fb06d67	Secondary	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	DECLARED	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected 9bb7e0f24e7e7d00daa1219b14539e2e602649b2 28d3551f8d8cb3aec7497894d94150fe84d20e5e gi
CNA	Linux	Linux	affected 9bb7e0f24e7e7d00daa1219b14539e2e602649b2 37e776e2e0a523731e2470dce6d563f0e8632a40 c
CNA	Linux	Linux	affected 9bb7e0f24e7e7d00daa1219b14539e2e602649b2 d32c07ef1880fe20cf4ab223dbfedc9c0b2816aa git
CNA	Linux	Linux	affected 9bb7e0f24e7e7d00daa1219b14539e2e602649b2 a1b7a843f12a0c3e9d3a2ca607ce451916ef42cf git
CNA	Linux	Linux	affected 9bb7e0f24e7e7d00daa1219b14539e2e602649b2 72b7ea786b8e570ae11149e9089859a4a8634a13
CNA	Linux	Linux	affected 9bb7e0f24e7e7d00daa1219b14539e2e602649b2 6dccbc9f3e1d38565dff7730d2b7d1e8b16c9b09 git
CNA	Linux	Linux	affected 5.0
CNA	Linux	Linux	unaffected 5.0 semver
CNA	Linux	Linux	unaffected 6.1.167 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.130 6.6.* semver
CNA	Linux	Linux	unaffected 6.12.78 6.12.* semver
CNA	Linux	Linux	unaffected 6.18.20 6.18.* semver
CNA	Linux	Linux	unaffected 6.19.10 6.19.* semver
CNA	Linux	Linux	unaffected 7.0 * original_commit_for_fix

References

Reference	Source	Link	Tags
git.kernel.org/stable/c/6dccbc9f3e1d38565dff7730d2b7d1e8b16c9b09	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/28d3551f8d8cb3aec7497894d94150fe84d20e5e	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/37e776e2e0a523731e2470dce6d563f0e8632a40	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/d32c07ef1880fe20cf4ab223dbfedc9c0b2816aa	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/a1b7a843f12a0c3e9d3a2ca607ce451916ef42cf	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/72b7ea786b8e570ae11149e9089859a4a8634a13	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
CVE Program record	CVE.ORG	www.cve.org	canonic

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)